

# SIMPLECRACKME.exe | crackmes.one

This is a simple crackme program that created for practice reverse engineering. But this is bit hard because not like previous one (acrackme.exe), This crackme haven't password as plain text. We need to patch this to get secret. So, let's get started.

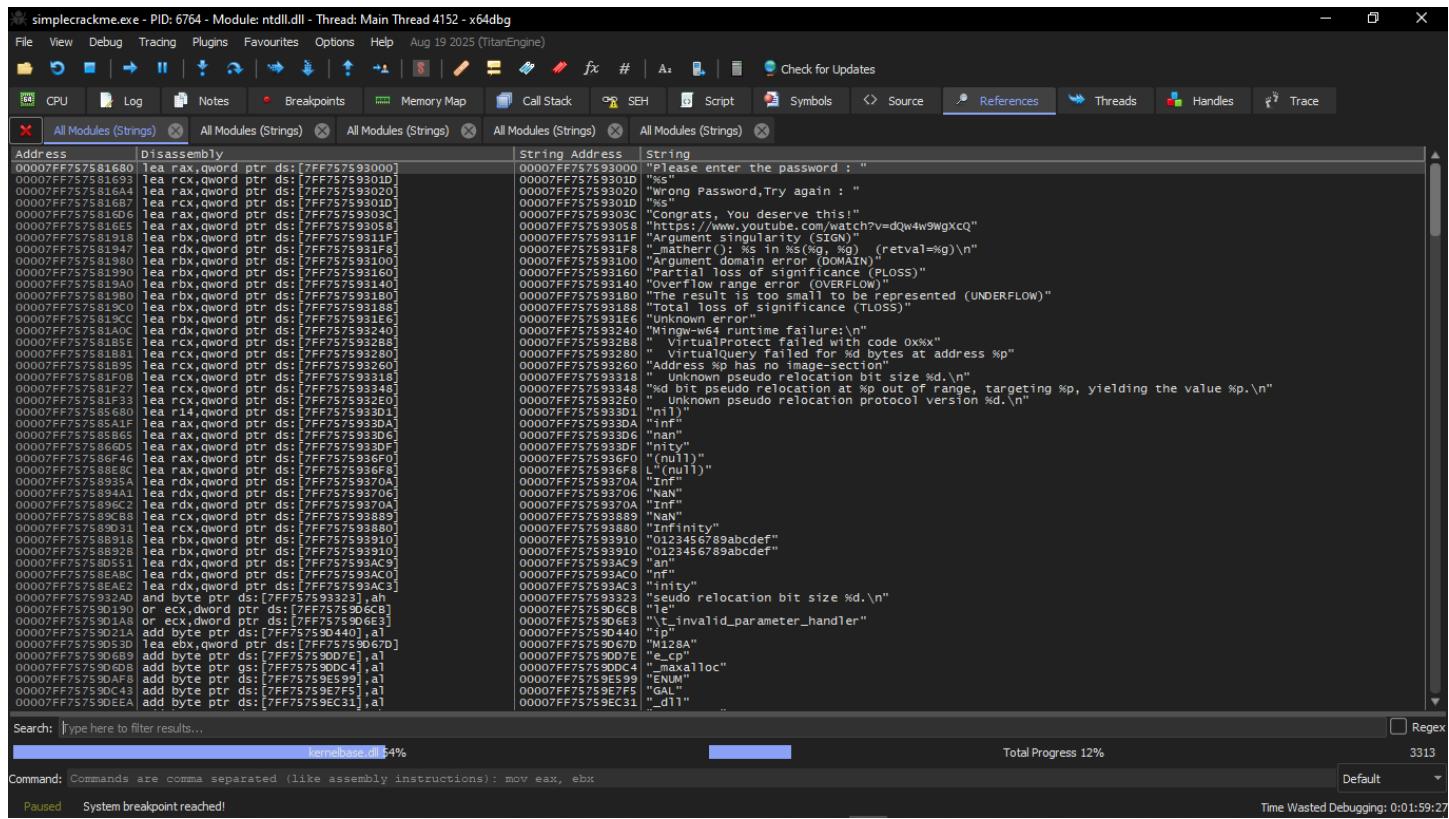
```
C:\Users\Piyusha Akash\Desktop\RevEng>dir
Volume in drive C has no label.
Volume Serial Number is 26D1-2522

Directory of C:\Users\Piyusha Akash\Desktop\RevEng

02/06/2026  01:56 PM    <DIR>        .
02/06/2026  01:56 PM    <DIR>        ..
02/04/2026  01:37 PM    <DIR>        Binary
02/06/2026  05:37 AM            3,786 crackme.cpp
01/03/2026  09:21 PM            66,048 crackme.exe
02/01/2026  10:35 PM           446,616 simplecrackme.exe
02/06/2026  01:52 PM    <DIR>        Writeups
              3 File(s)      516,450 bytes
              4 Dir(s)   39,441,752,064 bytes free

C:\Users\Piyusha Akash\Desktop\RevEng>simplecrackme.exe
Please enter the password : 123
Wrong Password,Try again :
```

So, as you can see, it will ask for password. So, I just entered "123" as a password and it is wrong and it will return "Wrong Password, Try again:" as the result. So, let's put this in to **x64 dbg** for analyze.



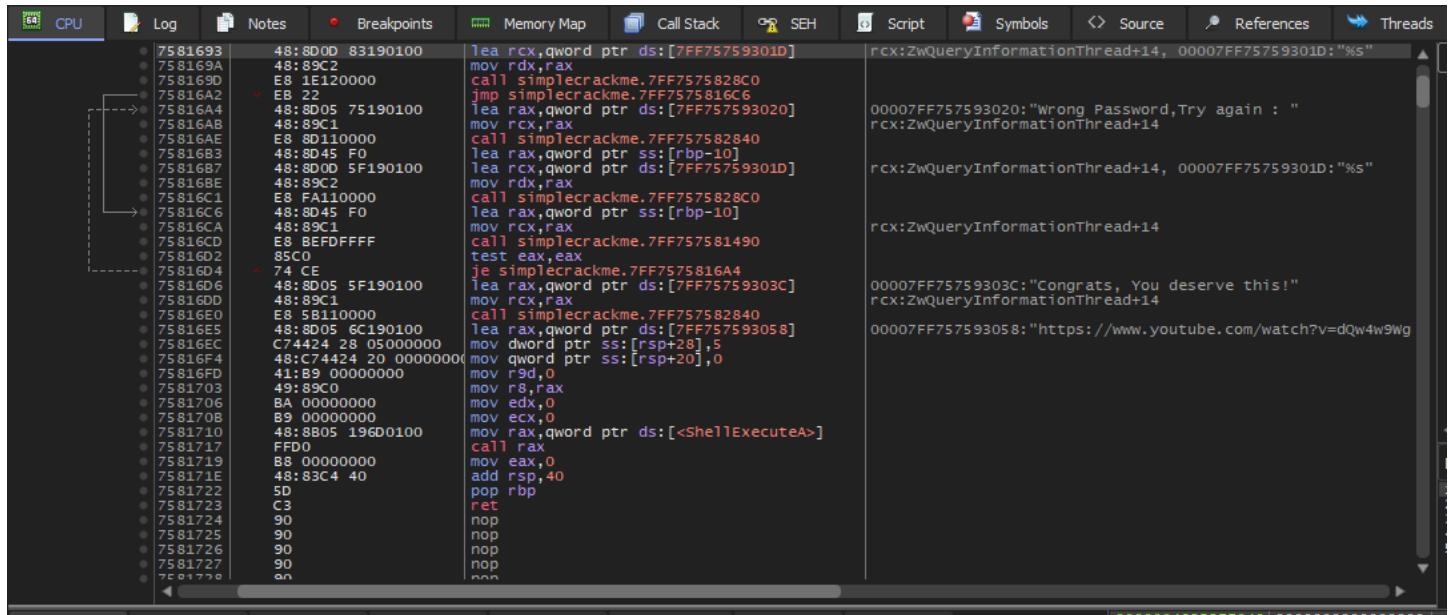
So, as you can see there is no any password as plaintext. We can see string "**Please enter the password:**" and input for password (**%s | %s is format specifier in C for string**) for example,

```
char password[10] = "";
```

```
printf("Please enter the password");
```

```
scanf("%s", password); // (This is an example code.)
```

So, let's jump to this section. I will double click this string and goes to disassembled section to looking for Assembly instructions.



So, you can see, the disassembled section. So, in that case, I don't care what is the password. As a hacker I have to make this program obey to my instructions. So, I just re-assemble the program by editing assembly instructions. Look at this image,

00007FF7575816CD	E8 BEFDFFFF	call simplecrackme.7FF757581490	
00007FF7575816D2	85C0	test eax,eax	
00007FF7575816D4	^ 74 CE	je simplecrackme.7FF7575816A4	00007FF75759303C:"Congrats, You deserve this!"
00007FF7575816D6	48:8D05 5F190100	lea rax,qword ptr ds:[7FF75759303C]	rcx:ZwQueryInformationThread+14
00007FF7575816D8	48:89C1	mov rcx,rax	
00007FF7575816E0	E8 5B110000	call simplecrackme.7FF757582840	
00007FF7575816E5	48:8D05 6C190100	lea rax,qword ptr ds:[7FF757593058]	00007FF757593058:"https://www.youtube.com/watch?v=dQw4w9Wg
00007FF7575816EC	C74424 28 05000000	mov dword ptr ss:[rsp+28],5	
00007FF7575816F4	48:C74424 20 00000000	mov qword ptr ss:[rsp+20],0	
00007FF7575816F8	41:B9 00000000	mov r9d,0	
00007FF757581703	49:89C0	mov r8,rax	
00007FF757581706	BA 00000000	mov edx,0	
00007FF757581708	B9 00000000	mov ecx,0	
00007FF757581710	48:8B05 196D0100	mov rax,qword ptr ds:[<ShellExecuteA>]	
00007FF757581717	FFD0	call rax	
00007FF757581719	B8 00000000	mov eax,0	
00007FF75758171E	48:83C4 40	add rsp,40	
00007FF757581722	5D	pop rbp	
00007FF757581723	C3	ret	
00007FF757581724	90	nop	
00007FF757581725	90	nop	
00007FF757581726	90	nop	
00007FF757581727	90	nop	
00007FF757581728	90	nop	

You can see a sting like "**Congrats, You deserve this!**". And you can see above to this string a "**je**" instruction. **JE** or **JZ**, whatever, It's meaning is "**Jump if equal**". So, according to the assembly instruction, If our password is true, Jump to

```
lea rax,qword ptr ds:[7FF75759303C]
```

```
00007FF75759303C:"Congrats, You deserve this!"
```

So, what if we can change the logic to if our password is wrong, jump to given memory address. So, let's try. I will change **je** to **jne**.

```
00007FF7575816D4
```

```
74 CE
```

```
je simplecrackme.7FF7575816A4
```

```
00007FF7575816D4
```

```
75 CE
```

```
jne simplecrackme.7FF7575816A4
```

Now assembly instructions are looks like this. So, I've changed **JE** to **JNE (Jump if Not Equal)**.

```

00007FF75758168F 48:8D45 F0 lea rax,qword ptr ss:[rbp-10]
00007FF757581693 48:8D0D 83190100 mov rcx,qword ptr ds:[7FF75759301D]
00007FF75758169A 48:89C2 mov rdx,rax
00007FF75758169D 48 1E120000 call simplecrackme.7FF7575828C0
00007FF7575816A2 < EB 22 jmp simplecrackme.7FF7575816C6
00007FF7575816A4 48:8D05 75190100 lea rax,qword ptr ds:[7FF757593020]
00007FF7575816AB 48:89C1 mov rcx,rax
00007FF7575816AE 48:8D10000 call simplecrackme.7FF757582840
00007FF7575816B3 48:8D45 F0 lea rax,qword ptr ss:[rbp-10]
00007FF7575816B7 48:8D0D 5F190100 lea rax,qword ptr ds:[7FF75759301D]
00007FF7575816BE 48:89C2 mov rdx,rax
00007FF7575816C1 48 FA110000 call simplecrackme.7FF7575828C0
00007FF7575816C6 48:8D45 F0 lea rax,qword ptr ss:[rbp-10]
00007FF7575816CA 48:89C1 mov rcx,rax
00007FF7575816CD 48 BEFDFFFF call simplecrackme.7FF757581490
00007FF7575816D2 85C0 test eax,eax
00007FF7575816D4 ^ 75 CE jne simplecrackme.7FF7575816A4
00007FF7575816D6 48:8D05 5F190100 lea rax,qword ptr ds:[7FF75759303C]
00007FF7575816D9 48:89C1 mov rcx,rax
00007FF7575816E0 48 5B110000 call simplecrackme.7FF757582840
00007FF7575816E5 48:8D05 6C190100 lea rax,qword ptr ds:[7FF757593058]
00007FF7575816EC C74424 28 05000000 mov dword ptr ss:[rsp+28],5
00007FF7575816F4 48:C74424 20 00000000 mov qword ptr ss:[rsp+20],0
00007FF7575816FD 41:B9 00000000 mov r9d,0
00007FF757581703 49:89C0 mov r8,rax
00007FF757581706 BA 00000000 mov edx,0
00007FF757581708 B9 00000000 mov ecx,0
00007FF757581710 48:8B05 196D0100 mov rax,qword ptr ds:[<ShellExecuteA>]
00007FF757581717 FFDD call rax
00007FF757581719 B8 00000000 mov eax,0
00007FF75758171E 48:83C4 40 add rsp,40
00007FF757581722 5D pop rbp
00007FF757581723 C3 ret
00007FF757581724 90 nop
00007FF757581725 90 nop
00007FF757581726 90 nop
00007FF757581727 90 nop

```

So, I will patch it using **CTRL+P** then save it as "**simplecrackme-cracked.exe**". So, let's execute our new PE file (Portable Execution file | .exe file).

```

C:\Windows\System32\cmd.exe

C:\Users\Piyusha Akash\Desktop\RevEng>dir
Volume in drive C has no label.
Volume Serial Number is 26D1-2522

Directory of C:\Users\Piyusha Akash\Desktop\RevEng

02/06/2026 02:35 PM <DIR> .
02/06/2026 02:35 PM <DIR> ..
02/04/2026 01:37 PM <DIR> Binary
02/06/2026 02:32 PM 68,120 Capture.PNG
02/06/2026 05:37 AM 3,786 crackme.cpp
01/03/2026 09:21 PM 66,048 crackme.exe
02/06/2026 02:35 PM 446,616 simplecrackme-cracked.exe
02/01/2026 10:35 PM 446,616 simplecrackme.exe
02/06/2026 02:21 PM <DIR> Writeups
      5 File(s)   1,031,186 bytes
      4 Dir(s) 39,421,612,032 bytes free

C:\Users\Piyusha Akash\Desktop\RevEng>simplecrackme-cracked.exe
Please enter the password : 1
Congrats, You deserve this!
C:\Users\Piyusha Akash\Desktop\RevEng>

```

So, it is successful. Now program has been cracked successfully. And it will open a YouTube link. We can also see that link while we looking for string.

Thank you for reading this writeup. Don't forget to follow me. Best regards, **Piyusha Akash. (0x3xp)**

Portfolio: <https://0x3xp.github.io>

LinkedIn: <https://linkedin.com/in/piyushaakash>

GitHub: <https://github.com/0x3xp>

Linktree: <https://linktr.ee/piyushaakash>